Approved for Release

Deborah A. Jefferson
Director for Human Resources
 Management

08/25/06
Date

DEPARTMENT OF COMMERCE
OFFICE OF HUMAN RESOURCES MANAGEMENT

HUMAN RESOURCES (HR) BULLETIN # 043, FY06

SUBJECT: Access to the National Finance Center (NFC) Payroll/Personnel Processing System

EFFECTIVE DATE: Upon release of this HR Bulletin

EXPIRATION DATE: Effective until canceled or superseded

SUPERSEDES: N/A

BACKGROUND: Since October 7, 2003, the National Finance Center (NFC) has been administratively suspending user IDs that are inactive for 60 or more days. To avoid future suspensions, please be sure the users in your bureau/office are signing on regularly to the NFC Mainframe system.

PURPOSE: The purpose of this HR bulletin is to describe the procedures for requesting access to the NFC system for new users, requesting modifications to access for current users (including un-suspending "Asuspended" IDs), and deleting access for those who no longer need it.

PROCEDURES: Each Servicing HR Manager should designate a Security Access Coordinator (SAC) and an alternate, and provide this information to the Departmental NFC Security Officer. All requests for new access, modifications, Asuspended IDs, or deletions must be submitted by the SAC or the Servicing HR Manager to the Departmental NFC Security Officer. Requests for new access and modifications (except un-suspending passwords) must be approved by the Servicing HR Manager. Access requests will be completed within 7 to 10 days of receipt by the Departmental NFC Security Officer unless the NFC staff needs further information to fulfill the request. SACs are delegated authority to un-suspend and change passwords for their respective submitting offices without further approval.

1. Requests are to be submitted to the Departmental NFC Security Officer via e-mail addressed to Naccess@doc.gov. The specific information described below must be included in the request. Incomplete requests will be returned to the originator.

2. Requests to establish new User IDs may be submitted when an employee first becomes responsible for work in your office requiring access to the NFC Payroll/Personnel Processing System. User IDs may not be carried from one operating personnel office to another as in the case of a reassignment or transfer. [In such instances, the losing office must request that the User ID be deleted and the gaining office must request that a new User ID be established.] Requests for new User IDs may not be submitted before the new user is in the NFC database for the new position.

3. Requests must include the user's first and last name, and social security number (SSNO). If the individual is a contractor, indicate "CONTRACTOR" in place of the SSNO and provide an expiration date. Indicate what the NFC ID prefix should be (e.g., CSxxx (Census), NNxxx (NOAA), etc.). Request specific profiles or applications. Be sure that you provide clear instructions of the type of access needed, e.g., IRIS/Non-sensitive or IRIS/Sensitive, TMGT/Update. Include the Agency Number and Personnel Office Identifier (POI). SACs should review NFC's Procedures Manual for the systems needed.

4. Access to sensitive data in PINQ and IRIS must be specifically identified and should only be requested if the new user needs to see such data as Race/National Origin Code, performance rating, handicap code, etc., for individual employees. The "Range of Access" must indicate whether the new user needs access to all bureaus serviced by a given HR office (provide bureau numbers and POI number), to an entire bureau regardless of servicing personnel office (provide bureau number only), or to only that part of a bureau serviced by a given HR office (provide bureau number and POI). The "Access Scope" must indicate whether the new user should be permitted to look at records only or if the user is authorized to add or change records. If access to FOCUS is requested, the library (PWAFOCUS) to be accessed must be indicated.

5. Requests to modify a user's access must include the user's complete name, current NFC ID, Agency, and POI. If the individual is a "contractor," and has been extended, indicate the new expiration date. Specify profiles or applications to be deleted or added, as indicated above.

6. Requests to change passwords and un-suspend User IDs should be directed to the organization's SAC. If the organization's SAC or alternate is not available, the Departmental NFC Security Officer may provide this service.

7. When a user leaves an office or is assigned to duties which no longer require access to the NFC system, the SAC must suspend the User ID immediately, and submit a request to delete the User ID. The user's complete name and NFC ID must be provided.

8. When requesting access to the NFC Reporting Center, please supply the user's complete name, social security number, NFC ID (if the user has one), Agency/POI, e-mail address, type of reports (workforce, personnel actions or financial reports),

organization structure and data type (detail sensitive or non-sensitive). Reporting Center access can be limited to the lowest level of an organization.

9. HR Managers should have their SACs attend NFC Security Officer Training. Information on training can be found in the NFC training catalog at http://dab.nfc.usda.gov/supportcenter/tcatalog/01training/secg.htm#g1.

REFERENCES: SACs should review the NFC security procedures manual at http://dab.nfc.usda.gov/pubs/na-pubsmain.html. Individual Systems Procedure Manuals for specific security access can be reviewed at http://dab.nfc.usda.gov/pubs/na-pubsmain.html.

OFFICE OF POLICY AND PROGRAMS: Felicia Purifoy, Director, fpurifoy@doc.gov, (202) 482-5291

PROGRAM MANAGER CONTACT INFORMATION: Marie Waters, mwaters3@doc.gov, (202) 482-0056

Marie Waters /HCHB/Osnet
08/24/2006 12:19 PM

To Darlene Armstrong/HCHB/Osnet@osnet

cc

bcc

Subject Fw: User Access to HRDSweb

FYI

----- Forwarded by Marie Waters/HCHB/Osnet on 08/24/2006 12:18 PM -----

Bill Fleming /HCHB/Osnet
08/18/2006 08:52 AM

To Marie Waters/HCHB/Osnet@osnet

cc Felicia Ann Purifoy/HCHB/Osnet@osnet, Thomas R
Kreider/HCHB/Osnet@osnet

Subject Re: Fw: User Access to HRDSweb

Let's update this document where needed (e.g., delete reference to PACT PRES for EPIC, etc.). How about putting it out as a HR Bulletin so that it is in our library. Many new folks may never know this type of guidance that was produced in letter form a few years ago, exists.

Thanks

Bill Fleming
OS/OHRM/DIR
US Dept of Commerce
202.482.4807
Marie Waters/HCHB/Osnet

Marie Waters /HCHB/Osnet
08/18/2006 08:29 AM

To Bill Fleming/HCHB/Osnet@osnet

cc Felicia Ann Purifoy/HCHB/Osnet@osnet, Thomas R
Kreider/HCHB/Osnet@osnet

Subject Fw: User Access to HRDSweb

NFC access is given to user by Bureau and POI, the only users who should have NFC access to all of Commerce are here in OHRM. Each Bureau has a Security Access Coordinator who receives NFC access request from their Servicing HR Manager. These request are forwarded to me to send to NFC. There are cases where a user from one POI may be given access to another POI, but the request and permission must come from the servicing HR office.

I have attached a copy of a Personnel/Payroll Processing Note, which describes the procedure for requesting access to NFC systems.

NOTE.094rev2.wpd

E. Marie Waters

Human Resources Specialist
U.S. Department of Commerce
O/S, OHRM
Office of Policy and Programs
Telephone: (202) 482-0056 Fax: (202) 482-3160
Internet: mwaters3@doc.gov
----- Forwarded by Marie Waters/HCHB/Osnet on 08/18/2006 07:50 AM -----

Felicia Ann Purifoy/ HCHB/ Osnet

08/18/2006 07:47 AM

To   "Marie Waters" <mWaters3@doc.gov>

cc

Subject   Fw: User Access to HRDSweb

Can you answer this please. Thanks.

Sent from my BlackBerry Wireless Handheld
    Thomas R Kreider

    From: Thomas R Kreider
    Sent: 08/17/2006 01:52 PM
    To: Bill Fleming
    Cc: Amy Woodling; Felicia Ann Purifoy; Gary Jacobs; Jeffery Wilkins; Linda
Kirton; Lorraine Shackelford; Sally Sheperd; Vidya Sagar
    Subject: Re: User Access to HRDSweb

Marie & Felica will have to address that.

Tom Kreider
OS/OHRM/HRIT
US Department of Commerce
(202)482-0537
Bill Fleming/HCHB/Osnet

Bill Fleming/HCHB/Osnet

08/17/2006 01:37 PM

To   Thomas R Kreider/HCHB/Osnet

cc   Amy Woodling/HCHB/Osnet@osnet, Felicia Ann Purifoy/HCHB/Osnet@osnet,
Gary Jacobs/HCHB/Osnet@osnet, Jeffery A Wilkins/HCHB/Osnet@osnet, Linda
Kirton/HCHB/Osnet@osnet, Lorraine Shackelford/HCHB/Osnet@osnet, Sally
Sheperd/HCHB/Osnet@osnet, Vidya Sagar/HCHB/Osnet@osnet

Subject   Re: User Access to HRDSweb

Same issue with access to NFC - what are our controls?

Bill Fleming
OS/OHRM/DIR
US Dept of Commerce
202.482.4807
Thomas R Kreider/HCHB/Osnet

Thomas
R
Kreider/
HCHB/
Osnet

08/17/2
006
01:32
PM

To Vidya Sagar/HCHB/Osnet@osnet

cc Amy Woodling/HCHB/Osnet@osnet, Gary Jacobs/HCHB/Osnet, Jeffery A
Wilkins/HCHB/Osnet@osnet, Lorraine Shackelford/HCHB/Osnet@Osnet, Sally
Sheperd/HCHB/Osnet@Osnet, Felicia Ann Purifoy/HCHB/Osnet@osnet, Linda
Kirton/HCHB/Osnet@osnet, Bill Fleming/HCHB/Osnet@osnet

Subject User Access to HRDSweb

Sagar,

During an unrelated discussion today with NOAA, it came to my attention that Chris Plestead has
universal access to all DOC employees in HRDSweb. She does not require this type of access, and it
should never have been granted. We must review the access levels for all users of HRDSweb to ensure
that this situation is not repeated elsewhere and is prevented from happening again.

I need for you to take the following steps.
1) Provide me a list of all HRDSweb accounts and span of access.
2) Create a Access Control Form for HRDSweb and let me see a draft by COB today.

This is a critical task. If we can't get the access correct very quickly, I'll side with caution and shut down
all access and start over.

Felicia, Linda, & Lorraine,
Not sure how you get the word out, but any new access requests must use this new form, and be signed
by the requestor, the requestor's HR director and Lorraine, only then will Sagar make the change. We will
most likely have to go out and document the current users too.

Tom Kreider
OS/OHRM/HRIT
US Department of Commerce
(202)482-0537

PERSONNEL/PAYROLL PROCESSING NOTE NO. 94
(REVISED)

MEMORANDUM FOR   Principal Human Resource Managers
Servicing Human Resource Managers
Security Access Coordinators

FROM: Fran White
Acting Director, Office of Compensation Innovation and
  Work Life Policy

SUBJECT: Access to the NFC Payroll/Personnel Processing System

The purpose of this Note is to describe the procedures for requesting access to the National Finance Center (NFC) system for new users, requesting modifications to access for current users (including un-suspending "Asuspended" IDs), and deleting access for those who no longer need it.

General

Each Servicing Human Resource Manager should designate a Security Access Coordinator (SAC) and an alternate, and provide this information to the Departmental NFC Security Officer. All requests for new access, modifications, Asuspended IDs, or deletions must be submitted by the SAC or the Servicing Human Resource Manager to the Departmental NFC Security Officer. Requests for new access and modifications (except un-suspending passwords) must be approved by the Servicing Human Resource Manager. Most access requests will be completed within seven to ten days of receipt by the Departmental NFC Security Officer unless the NFC staff needs further information to fulfill the request. SACs are delegated authority to un-suspend and change passwords for their respective submitting offices without further approval.

Since October 7, 2003, NFC will administratively suspend user ids that are inactive for 60 or more days. To avoid future suspensions, please be sure the users in your agency/department are signing on regularly to the NFC Mainframe system.

Requests are to be submitted to the Departmental NFC Security Officer via e-mail addressed to Naccess@doc.gov. The specific information described below must be included in the request. Incomplete requests will be returned to the originator.

New IDs

Requests to establish new User IDs may be submitted when an employee first becomes responsible for work in your office requiring access to the NFC Payroll/Personnel Processing System. User IDs may not be carried from one operating personnel office to another as in the case of a reassignment or transfer. [In such instances, the losing office must request that the User ID be deleted and the gaining office must request that a new User ID be established.] Requests for new User IDs may not be submitted before the new user is in the NFC database for the new position.

Requests must include the user's first and last name, and social security number (SSNO). If the individual is a contractor, indicate "CONTRACTOR" in place of the SSNO and provide an expiration date. Indicate what the NFC ID prefix should be (e.g., CSxxx (Census), NNxxx (NOAA), etc.). Request specific profiles or applications. Be sure that you provide clear instructions of the type of access needed, e.g., IRIS/Non-sensitive or IRIS/Sensitive, TMGT/Update. Include the Agency number and Personnel Office Identifier (POI). SACs should review NFC's Procedures manual for the systems needed.

Access to sensitive data in PINQ and IRIS must be specifically identified and should only be requested if the new user needs to see such data as Race/National Origin Code, performance rating, handicap code, etc., for individual employees. The "Range of Access" must indicate whether the new user needs access to all bureaus serviced by a given Human Resources office (provide bureau numbers and POI number), to an entire agency regardless of servicing personnel office (provide bureau number only), or to only that part of a bureau serviced by a given Human Resources office (provide bureau number and POI). The "Access Scope" must indicate whether the new user should be permitted to look at records only or if the user is authorized to add or change records. If access to FOCUS is requested, the library (PWAFOCUS) to be accessed must be indicated.

Modify Current IDs

Requests to modify a user's access must include the user's complete name, current NFC ID, Agency, and POI. If the individual is a "contractor," and has been extended, indicate the new expiration date. Specify profiles or applications to be deleted or added, as indicated above.

Requests to change passwords and un-suspend User IDs should be directed to the organization's SAC. If the organization's SAC or alternate is not available, the Departmental NFC Security Officer may provide this service.

Delete IDs

When a user leaves an office or is assigned to duties which no longer require access to the NFC system, the SAC must suspend the User ID immediately, and submit a request to delete the User ID. The user's complete name and NFC ID must be provided.

<u>Reporting Center</u>

When requesting access to the NFC Reporting Center, please supply the user's complete name, social security number, NFC ID (if the user has one), Agency/POI, e-mail address, type of reports (Workforce or Personnel Actions), organization structure and data type (detail sensitive or non-sensitive). Reporting Center access can be limited to the lowest level of an organization.

<u>Security Officers</u>

Human Resources Managers should have their SACs attend NFC Security Officer Training. Information on Training can be found in the NFC training catalog at http://dab.nfc.usda.gov/supportcenter/tcatalog/01training/secg.htm#g1. SACs should review the NFC security procedures manual at http://dab.nfc.usda.gov/pubs/na-pubsmain.html. Individual Systems Procedure Manuals for specific security access can be reviewed at http://dab.nfc.usda.gov/pubs/na-pubsmain.html.

Questions regarding this note or NFC access should be directed to Marie Waters, Departmental NFC Security Officer on 202-482-0056.

Filing Instructions: File with Title VI, Systems Access Manual; Chapter 1, Agency Liaison and Security Access; Section 1, Security Access.

OHRM:OCIWLP:MWaters:emw:05/25/04